

Claims

What is claimed is:

1. A parallel multiplier hardware architecture that delivers both a polynomial multiplication product with coefficients over $GF(2)$ and a natural multiplication product, the multiplier architecture comprising:

an array of AND gates with inputs connected to operand bits and with outputs providing a complete set of partial products of the operand bits, each partial product characterized by a bit significance or "weight";

an addition architecture arranged to add partial products of the same weight, the addition architecture constructed in multiple stages, a first group of stages arranged to add partial products without receiving any carry inputs from a lower weight portion of the addition architecture, a second group of stages arranged to add carry inputs from a lower weight portion of the addition architecture to results from previous stages, the stages in both groups providing carry outputs to a higher weight portion of the addition architecture; and

means connected between the first and second groups of stages for extracting the first stage addition result as a polynomial multiplication product, the natural multiplication product being extracted from the end of the second group of stages.

2. The multiplier architecture of claim 1 wherein the addition architecture comprises cascaded stages of parallel counters, with at least one counter in each column of partial products of the same weight, and wherein the means for extracting comprises bit lines connected to the least significant bit, representing polynomial product coefficients, from each first counter in the cascade.

3. The multiplier architecture of claim 1 wherein the addition architecture comprises a set of full adders arranged for adding the partial products and carries, each full adder receiving three inputs of equal weight and providing a sum output of the same weight and a carry output of next higher weight, a first group of adders not receiving any carry term as an input, the first group of adders arranged to reduce partial products of a given weight to a sum term, the means for extracting comprising bit lines connected to the sum terms representing polynomial product coefficients, the second group of adders receiving carry inputs and sum terms of a given weight and arranged to reduce the carry inputs and sum terms to natural product bits.

4. The multiplier architecture of claim 3 wherein the first group of adders includes at least one XOR gate reducing a pair of terms to one.

5. The multiplier architecture of claim 3 wherein the addition architecture also includes at least one half-adder connected to the first group of adders for reducing a pair of terms to one.

6. The multiplier architecture of claim 1 wherein the array of AND gates receive operand bits and provide partial products for more than one multiplication, and the addition architecture adds the partial products of the same weight from the more than one multiplication to provide both polynomial and natural multiplication results of the form $(\text{SUM}[A_i * B_i])$, where the A_i and B_i are the operands and any of the B_i operands can be one-word constants.

7. The multiple architecture of claim 6 wherein the addition architecture further adds to the partial products corresponding bits of identical weight of at least one accumulate or constant term to provide both polynomial and natural multiplication results of the form $(\text{SUM}[A_i * B_i] + \text{SUM}[C_i])$, where C_i, \dots are the accumulate or constant terms.

8. A method of multiplying two n-bit operands to obtain both a polynomial multiplication product with coefficients GF(2) and a natural multiplication product, the method comprising:

generating a complete set of partial products from operand bits, each partial product characterized by a bit significance or "weight" equal to the sum of the weights of the operand bits from which that partial product has been generated;

adding the partial products of the same weight in multiple stages of addition, a first group of stages adding the partial products without using any same weight carry results from lower weight additions, each addition generating a carry of next higher weight, a second group of stages adding sum results from the first group of stages with carry terms of the same weight; and

extracting polynomial product coefficients from the sum results obtained from the first group of stages of addition and extracting natural product bits from the sum results obtained from the second group of stages of addition.

9. The multiplication method of claim 8 wherein adding the partial products of the same weight comprises counting the number of partial products that have binary value 1 to provide a count value having a least significant bit of the same weight as the partial products counted and one or more higher significant bits of relatively higher weight, then repeating the counting step in a cascade of counting stages using the bits of the count values obtained from the preceding stage until a maximum of two bits of each weight remain, then performing a final addition operation with carries on the pairs of remaining bits to obtain the natural multiplication product; and

wherein extracting the polynomial product coefficients comprises extracting the least significant bits obtained from the first counting step.

10. The multiplication method of claim 8 wherein adding the partial products of the same weight is carried out solely with full adder circuits, each having three operand inputs, a sum output and a carry output.

11. The multiplication method of claim 8 wherein adding the partial products includes using at least one half-adder circuit in the first group of stages.

12. The multiplication method of claim 8 wherein extracting the polynomial product coefficients includes applying at least one XOR operation in the first group of stages.

13. The multiplication method of claim 8 wherein generating partial products from operand bits is conducted for more than one multiply operation, and wherein adding the partial products to obtain results for both polynomial product coefficients and natural product bits is also conducted for the more than one multiply operation, whereby the results have the form $(\text{SUM}[A_i * B_i])$, where the A_i and B_i are the operands and any of the B_i operands can be one-word constants.

14. The multiplication method of claim 13 wherein the adding step further includes adding to the partial products corresponding bits of identical weight of at least one accumulate or constant term to provide results for both polynomial product coefficients and natural product bits having the form $(\text{SUM}[A_i * B_i] + \text{SUM}[C_i])$ where the C_i, \dots are the accumulate or constant terms.